Rational points on $X_0^+(p^r)$

Yu. Bilu, P. Parent, M. Rebolledo

January 20, 2013

Abstract

We show how the recent isogeny bounds due to Gaudron and Rémond allow to obtain the triviality of $X_0^+(p^r)(\mathbb{Q})$, for $r > 1$ and p a prime exceeding $2 \cdot 10^{11}$. This includes the case of the curves $X_{\mathrm{split}}(p)$. We then prove, with the help of computer calculations, that the same holds true for p in the range $11 \le p \le 10^{14}$, $p \ne 13$. The combination of those results completes the qualitative study of such sets of rational points undertook in [4] and [5], with the exception of $p = 13$.

AMS 2010 Mathematics Subject Classification 11G18 (primary), 11G05, 11G16 (secondary).

To the memory of Fumiyuki Momose

1 Introduction

For p a prime number and $r > 1$ an integer, let $X_0(p^r)$ be the usual modular curve parameterizing geometric isomorphism classes of curves endowed with a cyclic isogeny of degree p^r, and let $X_0^+(p^r) := X_0(p^r)/w_p$ be its quotient by the Atkin-Lehner involution. When $r = 2s$ is even, $X_0^+(p^{2s})$ is $\mathbb{Q}$-isomorphic to the modular curve known as $X_{\mathrm{split}}(p^s)$. The curves $X_0^+(p^r)$ have motivated a number of works, dating back at least to Mazur's foundational paper [19], where the case of $X_{\mathrm{split}}(p)$ was tackled. Momose, among others, obtained important results in [23] and [24].

In [4, 5] we proved that for some absolute constant p_0, the only rational points of $X_0^+(p^r)$ with $p > p_0$ and $r > 1$ are trivial, that is, the unavoidable cusps and CM points. One easily checks the existence of degeneracy morphisms $X_0^+(p^{r+2}) \to X_0^+(p^r)$ which show it is sufficient to settle the cases $r = 2$ and 3 (see e.g. [24], p. 443). Our method uses three main ingredients: an integrality statement for non-cuspidal rational points (Mazur's method), an upper bound for the height of integral points (Runge's method), and a lower bound for the height of rational points (isogeny bounds, obtained by the transcendence methods). The combination of those yields inequalities of the following shape for the height of a (non-cuspidal and non-CM) rational point P:

$$c\,p < \mathrm{h}(P) < 2\pi\sqrt{p} + O(\log p) \qquad (r = 2), \tag{1}$$

$$c'p^{3/2} < \mathrm{h}(P) < 24p\log p + O(p) \qquad (r = 3), \tag{2}$$

where c and c' are positive constants. This of course yields a contradiction when p exceeds certain p_0, but the value for p_0 in [4, 5] was extremely large, due to the huge size of the constants $1/c$ and $1/c'$ furnished by the transcendence theory.

In previous works [26, 28] we had developed very different methods leading to the same triviality results for primes in certain congruence classes. We were not able to make those earlier techniques prove triviality of integral points for almost all primes; on the other hand, they are very fit for dealing with small primes p.

The aim of the present paper is therefore twofold. First we make the above inequalities (1) and (2) completely explicit. We did not try to obtain the numerical value of p_0 in [4, 5], but a calculation shows that in both cases triviality of $X_0^+(p^r)(\mathbb{Q})$ was established for p exceeding

10^{80} (which is supposed to be approximately the number of atoms in the visible universe). Now, thanks to the work of Gaudron and Rémond [12], who obtained drastic numerical improvements of classical isogeny bounds, we can size this down to the much more manageable $p \geq 1.4 \cdot 10^7$ for $r = 2$ and $p > 1.7 \cdot 10^{11}$ for $r = 3$.

The second aim of this article is then to develop an algorithm based on the Gross vectors method [26, 28] and to explain how to use it on a computer to rule out primes in the range $11 \leq p \leq 10^{14}$, $p \neq 13$. This results in the following theorem.

Theorem 1.1 *The points of $X_0^+(p^r)(\mathbb{Q})$ are trivial for all prime numbers $p \geq 11$, $p \neq 13$, and all integers $r > 1$.*

It is perhaps worth stressing here that, even if the help of a computer was forced by the important range of primes we had to consider, the computations themselves are very elementary, so that it takes only a few minutes to rule out a given prime by hand - even much beyond our bound 10^{14}. We refer the skeptical reader to Section 4.

For the remaining very small primes our methods break down, but ad hoc studies almost completely cleaned-up the situation, see [24, Theorem 3.6], [25, Theorems 0.1 and 3.14], and [11, Section 10]. Precisely:

- for $p = 2$ we have $X_0^+(2^r) \simeq \mathbb{P}^1$ for $2 \leq r \leq 5$ (the corresponding curves having thereby infinitely many $\mathbb{Q}$-points) and $X_0^+(2^r)(\mathbb{Q})$ is trivial for $r \geq 6$;
- for $p = 3$ we have $X_0^+(3^r) \simeq \mathbb{P}^1$ for $2 \leq r \leq 3$ and $X_0^+(3^r)(\mathbb{Q})$ is trivial for $r \geq 4$;
- for $p = 5$ we have $X_0^+(5^2) \simeq \mathbb{P}^1$, the curve $X_0^+(5^3)$ has one well-described non-trivial $\mathbb{Q}$-point [11, Section 10] and $X_0^+(5^r)(\mathbb{Q})$ is trivial for $r \geq 4$;
- for $p = 7$ we have $X_0^+(7^2) \simeq \mathbb{P}^1$ and $X_0^+(7^r)(\mathbb{Q})$ is trivial for $r \geq 3$;
- for $p = 13$ the set $X_0^+(13^r)(\mathbb{Q})$ is trivial for $r \geq 3$.

The only remaining question mark therefore concerns $X_0^+(13^2) \simeq X_{\text{split}}(13)$: this curve has genus 3 (so only a finite number of rational points) and Galbraith [10] or Baran [1] spotted seven (trivial) points, which they conjecture exhaust $X_0^+(13^2)(\mathbb{Q})$, but this still has to be checked... We continue this discussion of the level 13 case in Remark 4.10. On the other hand, the question for the curves $X_0^+(p)$ remains, as far as we know, essentially open, apart from some partial or experimental results (see for instance [10, 13]). In prime level our methods indeed fail for deep reasons akin to the ones that make the case of $X_{\text{nonsplit}}(p)$ so difficult (see, for instance, the introduction to [4]).

The problem of describing points over higher number fields is also extremely open (as it is a fortiori the case for the curves $X_0(N)$). As explained in [2, 3], one can explicitly bound integral and even S-integral points over arbitrary number field using Baker's method, but these bounds are quite huge and not very useful because of lack of integrality results. Finally, our techniques should at least partially extend to curves $X_0^+(N)$ where N has several prime factors (or even curves $X_0(N)/W$, where W is the full group generated by the Atkin-Lehner involutions, at least in the easier case where N is not square-free). We plan to pursue this study in forthcoming works.

Let us recall two immediate consequences of Theorem 1.1 for the arithmetic of elliptic curves. The first concerns Serre's uniformity problem over $\mathbb{Q}$ [30, 4]. Recall that to an elliptic curve over a field K and a prime number p (distinct from the characteristic of K) one associates the Galois representation $\rho_{E,p} : \text{Gal}(\bar{K}/K) \to \text{GL}(E[p]) \cong \text{GL}_2(\mathbb{F}_p)$. Serre [30] proved that, given a non-CM elliptic curve E defined over a number field K, there exists $p_0 = p_0(E, K)$ such that for $p > p_0$ the representation $\rho_{E,p}$ is surjective. He asked if p_0 can be made independent of E. In particular, in the case $K = \mathbb{Q}$ (which will be assumed in the sequel) it is widely believed that $p_0 = 37$ would do:

> *let E be a non-CM elliptic curve over $\mathbb{Q}$, and $p > 37$ a prime number; is it true that the associated Galois representation is surjective?*

As explained in the introduction of [4], to answer this question affirmatively it suffices to show that the image of the Galois representation is not contained in the normalizer of a (split or non-split) Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Since elliptic curves over $\mathbb{Q}$ for which the image of $\rho_{E,p}$ is contained in the normalizer of a split Cartan subgroup are parametrized by the $\mathbb{Q}$-points on the curve $X_{\mathrm{split}}(p) \simeq X_0^+(p^2)$ (see section 2), Theorem 1.1 has as immediate consequence the following improvement of the main result of [4].

Corollary 1.2 *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and p a prime number, $p \geq 11$, $p \neq 13$. Then the image of the Galois representation $\rho_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ is not contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.*

Another application of Theorem 1.1 concerns elliptic $\mathbb{Q}$-curves. Recall that an elliptic curve *with* complex multiplication, defined over $\bar{\mathbb{Q}}$, is isogenous to any of its conjugates (over $\mathbb{Q}$). A $\mathbb{Q}$-*curve* is an elliptic curve *without* complex multiplication over $\bar{\mathbb{Q}}$ with the same property, that is, which is isogenous to each of its conjugates over $\mathbb{Q}$. This notion was first introduced by Gross (in the setting of CM curves) in [14]; for more about this concept we refer in particular to the work of Elkies [8].

When a $\mathbb{Q}$-curve is *quadratic* (that is, defined over a quadratic field), we will say that it *has degree N* if there is a cyclic N-isogeny from the curve to its only non-trivial conjugate. For concrete examples of quadratic $\mathbb{Q}$-curves see for instance [11] and references therein.

It is known that quadratic $\mathbb{Q}$-curves of degree N are parametrized by the non-CM rational points of the curve $X_0^+(N)$, see [5, beginning of Section 7]. Hence Theorem 1.1 has the following consequence, improving on the main result of [5].

Corollary 1.3 *Let p be a prime number, $p \geq 11$ and $p \neq 13$. Then for $r > 1$ there does not exist quadratic $\mathbb{Q}$-curves of degree p^r.*

Plan of the article The material is organized as follows. In Section 2 we make the upper bounds in (1) and (2) explicit. In Section 3 we deduce the explicit lower bounds in (1) and (2) from the Gaudron-Rémond version of the isogeny theorem. The method and computations for small primes are explained in Section 4. Let us finally note that, due to the nature of our proofs, the cases $r = 2$ and $r = 3$ are not completely similar, so we often prefer deal with each case separately, at the expense of some repetitions.

Acknowledgments It is a pleasure to thank Éric Gaudron and Gaël Rémond for their efficiency in proving isogeny bounds which were even better than what they had promised, and for sharing their results with us. We are also grateful to the plafrim team in Bordeaux, who allowed us to make extensive computations on their machines, although what we eventually needed was less than we first feared.

While working on this article we learnt that Fumiyuki Momose had passed away, in April of 2010. His work has been a great source of inspiration for us, and we would like to dedicate this article to his memory.

Convention In this article we use the $O_1(\cdot)$-notation, which is a "quantitative version" of the familiar $O(\cdot)$-notation: $A = O_1(B)$ means $|A| \leq B$.

2 Explicit bounds for integral points

Recall that, to a positive integer N and a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, one associates a modular curve of level (dividing) N, denoted by X_G. In particular, when $N = p$ is a prime number, and G is the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ (for instance, the subgroup of diagonal and anti-diagonal elements), the corresponding curve will be denoted by $X_{\mathrm{split}}(p)$; it parametrizes geometric isomorphism classes of elliptic curves endowed with an unordered pair of independent

p-isogenies. For X_G any modular curve, we denote in the same way the Deligne-Rapoport model over $\mathbb{Z}$, and by Y_G the scheme deprived of the cusps.

In this section we prove the following explicit version of Theorem 1.1 from [4] (see Subsection 2.3).

Theorem 2.1 *For any prime number $p \geq 3$ and any $P \in Y_{\mathrm{split}}(p)(\mathbb{Z})$ we have*

$$\mathrm{h}(P) = \mathrm{h}(j_P) \leq 2\pi p^{1/2} + 6\log p + 21(\log p)^2 p^{-1/2}. \tag{3}$$

Here constants 2π and 6 are best possible for the method, but 21 can be refined, and can be replaced by 3 for sufficiently large p. The $\mathbb{Q}$-isomorphism $X_{\mathrm{split}}(p) \simeq X_0^+(p^2)$ shows that Theorem 2.1 allows to tackle the case $r = 2$ in Theorem 1.1. To deal with the case $r = 3$, we will further need a fully explicit version of Theorem 7.3 from [5] about integral points on $X_0(p^r)$, $r \geq 2$ (subsection 2.4). By the Faltings height $\mathrm{h}_{\mathcal{F}}(P)$ of a non-cuspidal point P on the curve $X_0(p^r)$ (or any modular curve) we mean the semi-stable Faltings height $\mathrm{h}_{\mathcal{F}}(E)$ of the underlying elliptic curve E (see [12], section 2.3, for a discussion on different normalization choices; our $\mathrm{h}_{\mathcal{F}}$ is the h_F of loc. cit.).

Theorem 2.2 *Let $p \geq 3$ be a prime number, K a quadratic number field with ring of integers $\mathcal{O}_K$, $r > 1$ an integer, and P a point of $Y_0(p^r)(\mathcal{O}_K)$. Then $\mathrm{h}_{\mathcal{F}}(P) \leq 2p\log p + 4p$.*

We follow the arguments of [4] and [5], making explicit all the implicit constants occurring therein. We shall routinely use the inequality[1]

$$\left|\log(1+z)\right| \leq -\frac{\log(1-r)}{r}|z| \qquad \text{for } |z| \leq r < 1. \tag{4}$$

2.1 Siegel Functions

We denote by $\mathcal{H}$ the Poincaré upper half-plane and put $\bar{\mathcal{H}} = \mathcal{H} \cup \mathbb{Q} \cup \{i\infty\}$. For $\tau \in \mathcal{H}$ we, as usual, put $q = q(\tau) = e^{2\pi i\tau}$. For a rational number a we define $q^a = e^{2\pi i a\tau}$. Let $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2$ be such that $\mathbf{a} \notin \mathbb{Z}^2$, and let $g_{\mathbf{a}} : \mathcal{H} \to \mathbb{C}$ be the corresponding *Siegel function* [17, Section 2.1]. Then we have the following infinite product presentation for $g_{\mathbf{a}}$ [17, page 29]:

$$g_{\mathbf{a}}(\tau) = -q^{B_2(a_1)/2} e^{\pi i a_2(a_1-1)} \prod_{n=0}^{\infty} \left(1 - q^{n+a_1} e^{2\pi i a_2}\right)\left(1 - q^{n+1-a_1} e^{-2\pi i a_2}\right), \tag{5}$$

where $B_2(T) = T^2 - T + 1/6$ is the second Bernoulli polynomial.

The following is a quantitative version of (slightly modified) Proposition 2.1 from [4]. Let D be the familiar fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$ (that is, the hyperbolic triangle with vertices $e^{\pi i/3}$, $e^{2\pi i/3}$ and $i\infty$, together with the geodesic segments $[i, e^{2\pi i/3}]$ and $[e^{2\pi i/3}, i\infty]$) and $D + \mathbb{Z}$ the union of all translates of D by the rational integers.

Proposition 2.3 *Assume that $0 \leq a_1 < 1$. Then for $\tau \in D + \mathbb{Z}$ we have*

$$\log|g_{\mathbf{a}}(\tau)| = \frac{1}{2}B_2(a_1)\log|q| + \log\left|1 - q^{a_1}e^{2\pi i a_2}\right| + \log\left|1 - q^{1-a_1}e^{-2\pi i a_2}\right| + O_1(3|q|).$$

Proof We only have to show that

$$\left|\sum_{n=1}^{\infty}\left(\log\left|1 - q^{n+a_1}e^{2i\pi a_2}\right| + \log\left|1 - q^{n+1-a_1}e^{-2i\pi a_2}\right|\right)\right| \leq 3|q|.$$

But this is inequality (11) from [5]. We may notice that in [5] it is assumed that $\tau \in D$, but what is actually used is the inequality $|q(\tau)| \leq e^{-\pi\sqrt{3}}$, which holds for every $\tau \in D + \mathbb{Z}$. □

[1] We choose the principal determination of the logarithm, that is, for $z \in \mathbb{C}$ satisfying $|z| < 1$, we set $\log(1+z) := -\sum_{k=1}^{\infty}(-z)^k/k$.

2.2 A Modular Unit

In this subsection we briefly recall the "modular unit" construction. See [4, Section 3] for more details.

Let N be a positive integer. Then for $\mathbf{a}, \mathbf{a}' \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$ such that $\mathbf{a} \equiv \mathbf{a}' \mod \mathbb{Z}^2$, we have $g_{\mathbf{a}}^{12N} = g_{\mathbf{a}'}^{12N}$. Hence the function $g_{\mathbf{a}}^{12N}$ is well-defined for $\mathbf{a}$ in $\big(N^{-1}\mathbb{Z}/\mathbb{Z}\big)^2 \smallsetminus \{0\}$. The function $u_{\mathbf{a}} = g_{\mathbf{a}}^{12N}$ is $\Gamma(N)$-automorphic and hence defines a rational function on the modular curve $X(N)(\mathbb{C})$; in fact, it belongs to the field $\mathbb{Q}(\zeta_N)\big(X(N)\big)$.

Now assume that $N = p \geq 3$ is an odd prime number, and denote by $p^{-1}\mathbb{F}_p^\times$ the set of non-zero elements of $p^{-1}\mathbb{Z}/\mathbb{Z}$. Put

$$A = \big\{(a,0) : a \in p^{-1}\mathbb{F}_p^\times\big\} \cup \big\{(0,a) : a \in p^{-1}\mathbb{F}_p^\times\big\}, \qquad U = \prod_{\mathbf{a}\in A} u_{\mathbf{a}}.$$

Then U is $\Gamma_{\mathrm{split}}(p)$-automorphic; in particular, it defines a rational function on $X_{\mathrm{split}}(p)$, also denoted by U; in fact, $U \in \mathbb{Q}(X_{\mathrm{split}}(p))$.

More generally, for $c \in \mathbb{Z}$ put

$$\beta_c = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \qquad U_c = U \circ \beta_c = \prod_{\mathbf{a}\in A\beta_c} u_{\mathbf{a}}$$

(recall that $u_{\mathbf{a}} \circ \gamma = u_{\mathbf{a}\gamma}$), so that $U = U_0$. (Warning: for c non-divisible by p the function U_c is not $\Gamma_{\mathrm{split}}(p)$-automorphic!) The following is a quantitative version of Proposition 3.3 from [4].

Proposition 2.4 *For $\tau \in D + \mathbb{Z}$ we have*

$$\log|U_c(\tau)| = \begin{cases} (p-1)^2 \log|q| + O_1\left(4\pi^2 \dfrac{p^2}{\log|q^{-1}|} + 12p\log p + 77p^2|q|\right) & \text{if } p \mid c, \\ -2(p-1)\log|q| + O_1\left(8\pi^2 \dfrac{p^2}{\log|q^{-1}|} + 72p^2|q|\right) & \text{if } p \nmid c, \end{cases}$$

where we write $q = q(\tau)$.

For the proof of Proposition 2.4 we need a slight sharpening of Lemma 3.5 from [4].

Lemma 2.5 *Let z be a complex number, $|z| < 1$, and N a positive integer. Then*

$$\left|\sum_{k=1}^{N} \log\big|1 - z^k\big|\right| \leq \frac{\pi^2}{6} \frac{1}{\log|z^{-1}|}. \tag{6}$$

Proof We have $\big|\log|1+z|\big| \leq -\log(1-|z|)$ for $|z| < 1$. Hence it suffices to prove the inequality

$$-\sum_{k=1}^{\infty} \log(1-q^k) \leq \frac{\pi^2}{6} \frac{1}{\log(q^{-1})} \qquad (\text{for } 0 < q < 1). \tag{7}$$

Using (4) with q instead of z and with $r = 1/2$, we find that for $0 < q \leq 1/2$

$$-\sum_{k=1}^{\infty} \log(1-q^k) \leq (4\log 2)q \leq \frac{4\log 2}{e} \frac{1}{\log(q^{-1})} < \frac{\pi^2}{6} \frac{1}{\log(q^{-1})},$$

which proves (7) for $0 < q \leq 1/2$. We are left with $1/2 \leq q < 1$.

Put $\tau = \log q/(2\pi i)$. Then

$$-\sum_{k=1}^{\infty} \log(1-q^k) = \frac{1}{24}\log q - \log|\eta(\tau)|,$$

where $\eta(\tau)$ is the Dedekind η-function. Since $|\eta(\tau)| = |\tau|^{-1/2}|\eta(-\tau^{-1})|$, we have

$$-\sum_{k=1}^{\infty}\log(1-q^k) = -\frac{1}{24}\log Q + \frac{1}{24}\log q + \frac{1}{2}\log|\tau| - \sum_{k=1}^{\infty}\log(1-Q^k) \tag{8}$$

with $Q = e^{-2\pi i\tau^{-1}} = e^{4\pi^2/\log q}$. The first term on the right of (8) is exactly $(\pi^2/6)/\log(q^{-1})$, and the second term is negative for $0 < q < 1$. To complete the proof, we must show that, when $1/2 \le q < 1$, the sum of the remaining two terms is negative.

Indeed, when $1/2 \le q < 1$, we have

$$\frac{1}{2}\log|\tau| \le -\frac{1}{2}\log\frac{2\pi}{\log 2} \le -1, \qquad Q \le e^{-4\pi^2/\log 2} \le 10^{-24}.$$

Applying (4) with Q instead of z and with $r = 10^{-24}$, we bound the fourth term in (8) by 10^{-23}. Hence the sum of the third and the fourth terms is negative, as wanted. □

Proof of Proposition 2.4 For $a \in \mathbb{Q}/\mathbb{Z}$ we denote by $\tilde{a}$ the lifting of a to the interval $[0,1)$. Then for $\tau \in D + \mathbb{Z}$ we deduce from Proposition 2.3 that

$$\log|U_c(\tau)| = 6p\Sigma_1\log|q| + 12p\Sigma_2 + O_1(72p^2|q|), \tag{9}$$

where

$$\Sigma_1 = \sum_{\mathbf{a}\in A\beta_c} B_2(\tilde{a}_1), \qquad \Sigma_2 = \sum_{\mathbf{a}\in A\beta_c}\Big(\log\big|1-q^{\tilde{a}_1}e^{2\pi i a_2}\big| + \log\big|1-q^{1-\tilde{a}_1}e^{-2\pi i a_2}\big|\Big).$$

Now we are going to calculate Σ_1, using the identity

$$\sum_{k=1}^{N-1} B_2\left(\frac{k}{N}\right) = -\frac{(N-1)}{6N},$$

and to estimate Σ_2 using Lemma 2.5.

If $p \mid c$ then $A\beta_c = A$ and

$$\Sigma_1 = \sum_{k=1}^{p-1} B_2\left(\frac{k}{p}\right) + (p-1)B_2(0) = \frac{(p-1)^2}{6p}, \tag{10}$$

$$\Sigma_2 = 2\sum_{k=1}^{p-1}\log\big|1-q^{k/p}\big| + \log\left|\frac{1-q^p}{1-q}\right| + \log p. \tag{11}$$

Lemma 2.5 with $z = q^{1/p}$ implies that

$$\Big|\sum_{k=1}^{p-1}\log|1-q^{k/p}|\Big| \le \frac{\pi^2}{6}\frac{p}{\log|q^{-1}|}.$$

Also, since $|q| \le e^{-\pi\sqrt{3}}$, we have $\Big|\log|1-q|\Big| \le 1.01|q|$ and $\Big|\log|1-q^p|\Big| \le 1.01|q|^p \le 0.01|q|$. Combining all this with (9), (10) and (11), we prove the proposition in the case $p \mid c$.

If $p \nmid c$ then $A\beta_c = \{(a,0) : a \in p^{-1}\mathbb{F}_p^\times\} \cup \{(a,ab) : a \in p^{-1}\mathbb{F}_p^\times\}$, where $bc \equiv 1 \bmod p$. Hence

$$\Sigma_1 = 2\sum_{k=1}^{p-1} B_2\left(\frac{k}{p}\right) = -\frac{p-1}{3p},$$

$$\Sigma_2 = 2\sum_{k=1}^{p-1}\log\big|1-q^{k/p}\big| + 2\sum_{k=1}^{p-1}\log\big|1-(q^{1/p}e^{2\pi ib/p})^k\big|.$$

Using Lemma 2.5 with $z = q^{1/p}$ and with $z = q^{1/p}e^{2\pi ib/p}$, we complete the proof. □

2.3 Proof of Theorem 2.1

We set G as the subgroup of diagonal and anti-diagonal matrices in $\mathrm{GL}_2(\mathbb{F}_p)$ and choose the corresponding modular curve as a model for $X_{\mathrm{split}}(p)$. Define the "modular units" U_c as in Subsection 2.2. Recall that $U = U_0$ belongs to the field $\mathbb{Q}(X_{\mathrm{split}}(p))$. Theorem 2.1 is a consequence of Proposition 2.4 and the following statement, which is Proposition 4.2 from [4].

Proposition 2.6 *For $P \in Y_{\mathrm{split}}(p)(\mathbb{Z})$ we have $0 \leq \log|U(P)| \leq 24p\log p$.* □

We are ready now to prove Theorem 2.1. Let $p \geq 3$ and $P \in Y_{\mathrm{split}}(p)(\mathbb{Z})$. According to Lemma 3.2 from [4], there exists $\tau \in D + \mathbb{Z}$ and $c \in \mathbb{Z}$ with $U_c(\tau) = U(P)$ and $j(\tau) = j(P)$. We write $q = q(\tau)$. Recall that $j(\tau)$ and $q(\tau)$ are real numbers, and that $\mathrm{h}(j(\tau)) = \log|j(\tau)|$ if $j(\tau) \in \mathbb{Z}$. It suffices to show that

$$\log|q^{-1}| \leq 2\pi p^{1/2} + 6\log p + 20(\log p)^2 p^{-1/2}. \tag{12}$$

Indeed, we may assume that $|j(\tau)| \geq 3500$ (otherwise (3) holds trivially), in which case Corollary 2.2 of [5] gives $\left|j(\tau) - q^{-1}\right| \leq 1100$. Hence, using the inequality

$$\log|a| \leq \log|b| + \frac{|a-b|}{|a| - |a-b|},$$

which holds for real numbers a and b with same sign (and $0 < |b| < |a|$ or $0 < |a| < |b| < |2a|$), we obtain

$$\log|j(\tau)| \leq \log|q^{-1}| + \frac{1100}{|j(\tau)| - 1100}.$$

Now using (12) and assuming that $\log|j(\tau)| \geq 2\pi p^{1/2} + 6\log p$, we obtain

$$\log|j(\tau)| \leq 2\pi p^{1/2} + 6\log p + 20\frac{(\log p)^2}{p^{1/2}} + \frac{1100}{p^6 e^{2\pi p^{1/2}} - 1100} \leq 2\pi p^{1/2} + 6\log p + 21\frac{(\log p)^2}{p^{1/2}},$$

as wanted.

Let us prove (12). Assume first that $p \nmid c$. Using Propositions 2.4 and 2.6 and assuming that $\log|q^{-1}| \geq 2\pi p^{1/2} + 6\log p$, we obtain

$$\begin{aligned}
\log|q^{-1}| &\leq \frac{\log|U_c(\tau)|}{2(p-1)} + \frac{4\pi^2 p^2}{p-1}\frac{1}{\log|q^{-1}|} + 36\frac{p^2}{p-1}|q| \\
&\leq \frac{12p\log p}{p-1} + \frac{4\pi^2 p}{\log|q^{-1}|} + \frac{4\pi^2 p}{p-1}\frac{1}{\log|q^{-1}|} + 54p|q| \\
&\leq 12\log p + \frac{12\log p}{p-1} + \frac{4\pi^2 p}{\log|q^{-1}|} + \frac{2\pi p^{1/2}}{p-1} + 54p^{-5}e^{-2\pi p^{1/2}} \\
&\leq 12\log p + \frac{4\pi^2 p}{\log|q^{-1}|} + \frac{21}{p^{1/2}}.
\end{aligned}$$

It follows that $\log|q^{-1}|$ does not exceed the largest root of the quadratic polynomial

$$f(T) = T^2 - \left(12\log p + 21p^{-1/2}\right)T - 4\pi^2 p,$$

that is,

$$\begin{aligned}
\log|q^{-1}| &\leq \left(4\pi^2 p + \left(6\log p + 10.5p^{-1/2}\right)^2\right)^{1/2} + 6\log p + 10.5p^{-1/2} \\
&\leq 2\pi p^{1/2} + \frac{\left(6\log p + 10.5p^{-1/2}\right)^2}{4\pi p^{1/2}} + 6\log p + 10.5p^{-1/2} \qquad (13) \\
&\leq 2\pi p^{1/2} + 6\log p + 20(\log p)^2 p^{-1/2},
\end{aligned}$$

where we use the inequality $(a+b)^{1/2} \le a^{1/2} + (1/2)ba^{-1/2}$ in (13). This completes the proof of (12) in the case $p \nmid c$.

In the case $p \mid c$ Proposition 2.4 gives

$$\log|q^{-1}| \le -\frac{\log|U_c(\tau)|}{(p-1)^2} + \frac{4\pi^2 p^2}{(p-1)^2}\frac{1}{\log|q^{-1}|} + \frac{12p\log p}{(p-1)^2} + \frac{77p^2}{(p-1)^2}|q|.$$

Proposition 2.6 implies that $-\log|U_c(\tau)| \le 0$. Assuming that $\log|q^{-1}| \ge 2\pi p^{1/2} + 6\log p$, we obtain

$$\log|q^{-1}| \le \frac{2\pi p^{3/2}}{(p-1)^2} + \frac{12p\log p}{(p-1)^2} + \frac{77}{(p-1)^2 p^4}e^{-2\pi p^{1/2}} \le 19,$$

which is sharper than (12). The theorem is proved. □

2.4 Integral points on $X_0(p^r)$: proof of Theorem 2.2

Let p be a prime number as usual. We will use the following double-covering of $X_{\mathrm{split}}(p)$. Let denote by $X_{\mathrm{sp.C}}(p)$ the curve corresponding to a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ (*not* its normalizer), for instance the diagonal subgroup (see the beginning of Section 2). It parametrizes geometric isomorphism classes of elliptic curves endowed with an *ordered* pair of independent p-isogenies. Factorizing by the natural involution that switches the isogenies (which is induced by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ acting on the Poincaré half-plane $\mathcal{H}$) defines a degree-2 covering $X_{\mathrm{sp.C}}(p) \to X_{\mathrm{split}}(p)$. On the other hand, there is an isomorphism $\phi : X_0(p^2) \to X_{\mathrm{sp.C}}(p)$ over $\mathbb{Q}$ defined functorially as

$$\big(E, A\big) \mapsto \big(E/B, (B^*, C)\big), \tag{14}$$

where $A = C \circ B$ is the obvious decomposition of the cyclic p^2-isogeny A into the product of two p-isogenies and B^* is the dual isogeny. On the Poincaré upper half-plane $\mathcal{H}$, the map ϕ is induced by $\tau \mapsto p\tau$.

This interplay between the isomorphic curves might look a bit confusing at first sight, but each point of view has its own advantages. In particular, replacing $X_0(p^2)$ by $X_{\mathrm{sp.C}}(p)$ (that is, a level p^2-structure by a p-structure) is significantly more advantageous for Runge's method.

Furthermore, curves $X_0^+(p^2)$ and $X_{\mathrm{split}}(p)$ are quotients of $X_0(p^2)$ and $X_{\mathrm{sp.C}}(p)$, respectively, by natural involutions, and a straightforward verification shows that (14) defines a $\mathbb{Q}$-isomorphism $X_0^+(p^2) \to X_{\mathrm{split}}(p)$.

We deduce Theorem 2.2 from the following result, which is Theorem 6.1 from [5].

Theorem 2.7 *Let $p \ge 3$ be a prime number and K a number field of degree at most 2. Then for a point $P \in Y_{\mathrm{sp.C}}(p)(\mathcal{O}_K)$ we have $\mathrm{h}(P) \le 24p\log(3p)$.*

We shall need some basic estimates concerning the Faltings height.

Proposition 2.8 *(i) Let E and E' be isogenous elliptic curves over some number field, connected by an isogeny of degree δ. Then $|\mathrm{h}_{\mathcal{F}}(E) - \mathrm{h}_{\mathcal{F}}(E')| \le (1/2)\log\delta$.*

(ii) For an elliptic curve E we have $\mathrm{h}_{\mathcal{F}}(E) \le (1/12)\mathrm{h}(j_E) + 3$.

Item (i) is a well-known result of Faltings [9, Lemma 5]. Item (ii) is, basically, due to Silverman [31, Proposition 2.1], who proved the inequality $\mathrm{h}_{\mathcal{F}}(E) \le (1/12)\mathrm{h}(j_E) + C$ with an unspecified absolute constant C. The calculations of Pellarin on pages 240–241 of [27] imply that $C = 4$ would do, though he does not state this explicitly. It finally follows from Gaudron and Rémond [12, Lemma 7.9] that $C = 3$ would do.

Proof of Theorem 2.2 We may assume $r = 2$. Let $\phi : X_0(p^2) \to X_{\mathrm{sp.C}}(p)$ be the isomorphism defined by (14). Then the elliptic curve implied by a point P on $X_0(p^2)$ is p-isogenous to the curve implied by the point $P' = \phi(P)$ on $X_{\mathrm{sp.C}}(p)$. Proposition 2.8 implies that

$$\mathrm{h}_{\mathcal{F}}(P) \le \mathrm{h}_{\mathcal{F}}(P') + \frac{1}{2}\log p, \qquad \mathrm{h}_{\mathcal{F}}(P') \le \frac{1}{12}\mathrm{h}(P') + 3.$$

Finally, Theorem 2.7 applied to the point P' gives $\mathrm{h}(P') \le 24p\log(3p)$. Combining all this, we obtain

$$\mathrm{h}_{\mathcal{F}}(P) \le 2p\log(3p) + \frac{1}{2}\log p + 3 \le 2p\log p + 4p,$$

as wanted. □

3 An Upper Bound for p

The main result of this section is Theorem 3.2. It is an explicit version of Theorem 1.3 from [5], which covers Theorem 1.2 from [4]. Our previous work relied on Pellarin's refinement [27] of Masser-Wüstholz famous upper bound [18] for the smallest degree of an isogeny between two elliptic curves. Here we invoke the very recent improvement on Pellarin's bound, due to Gaudron and Rémond [12, Theorem 1.4], with much sharper numerical constants.

Theorem 3.1 (Gaudron and Rémond) *Let E be an elliptic curve defined over a number field K of degree d. Let E' be another elliptic curve, defined over K and isogenous to E over $\bar{K}$. Then there exists an isogeny $\psi : E \to E'$ of degree at most $10^7 d^2\big(\max\{\mathrm{h}_{\mathcal{F}}(E), 985\} + 4\log d\big)^2$.*

We combine Theorems 2.1, 2.2 and 3.1 to prove the following.

Theorem 3.2 *(i) For $p > 1.4 \cdot 10^7$, every point in $X_0^+(p^2)(\mathbb{Q})$ is either a CM point or a cusp.*

(ii) For $p > 1.7 \cdot 10^{11}$, every point in $X_0^+(p^3)(\mathbb{Q})$ is either a CM point or a cusp.

A numerically sharper version of item (i) is also given in [12]. Our version is sufficient for our purposes.

We shall use Theorem 3.1 through its following immediate consequence.

Proposition 3.3 *Let E be a non-CM elliptic curve defined over a number field K of degree d, and admitting a cyclic isogeny over K of degree δ. Then $\delta \le 10^7 d^2\big(\max\{\mathrm{h}_{\mathcal{F}}(E), 985\} + 4\log d\big)^2$.*

Proof Let ϕ be a cyclic isogeny from E to E'. Let $\psi\colon E \to E'$ be an isogeny of degree bounded by $10^7 d^2 \max\big(\mathrm{h}_{\mathcal{F}}(E) + 4\log d, 10^3\big)^2$ granted by Theorem 3.1, and let $\psi^*\colon E' \to E$ be the dual isogeny. As E has no CM, the composed map $\psi^* \circ \phi$ must be multiplication by some integer n and then $n^2 = \deg(\phi)\deg(\psi)$. Since ϕ is cyclic, $\deg(\phi) \le |n|$. It follows that $\deg(\phi) \le \deg(\psi)$ or $\deg(\phi) = |n|$ and $\phi = \pm\psi$. □

Proof of Theorem 3.2 We start with item (i). Let Q be a non-cuspidal and non-CM point in $X_0^+(p^2)(\mathbb{Q})$, and let P be the corresponding point in $X_{\mathrm{split}}(p)(\mathbb{Q})$ defined by (14). Let E_1 and E_2 be the elliptic curves corresponding to Q (defined over a quadratic extension of $\mathbb{Q}$) and let E be the elliptic curve associated with P.

Since E and E_1 are p-isogenous, Proposition 2.8 implies that

$$\mathrm{h}_{\mathcal{F}}(E_1) \le \mathrm{h}_{\mathcal{F}}(E) + \frac{1}{2}\log p \le \frac{1}{12}\mathrm{h}(j_E) + \frac{1}{2}\log p + 3. \tag{15}$$

A result of Mazur, Momose and Merel (see Theorem 6.1 in [4]) implies that $j(P) = j_E \in \mathbb{Z}$; in particular, $\mathrm{h}(j_E) = \log|j_E|$. Hence we may use Theorem 2.1, which yields

$$\frac{1}{12}\mathrm{h}(j_E) \leq \frac{2\pi}{12}p^{1/2} + \frac{1}{2}\log p + \frac{21}{12}\frac{(\log p)^2}{p^{1/2}}. \tag{16}$$

On the other hand, since the curve E_1 admits a cyclic p^2-isogeny over a quadratic field, Proposition 3.3 implies that $p^2 \leq 4\cdot 10^7\big(\max\{\mathrm{h}_{\mathcal{F}}(E_1), 985\} + 4\log 2\big)^2$. It follows that $p \leq 7\cdot 10^3 \max\{\mathrm{h}_{\mathcal{F}}(E_1), 985\}$, that is, either $p \leq 7\cdot 10^6$ and we are done, or $p \leq 7\cdot 10^3 \mathrm{h}_{\mathcal{F}}(E_1)$. In this latter case, using (15) and (16), we obtain

$$p \leq 7\cdot 10^3\left(\frac{2\pi}{12}p^{1/2} + \log p + 3 + \frac{21}{12}\frac{(\log p)^2}{p^{1/2}}\right). \tag{17}$$

One readily checks that for $p \geq 10^7$ the right-hand side of (17) does not exceed $3.71\cdot 10^3 p^{1/2}$, which implies that $p \leq 1.4\cdot 10^7$. This proves item (i).

For the proof of item (ii) we play the same game, in a more straightforward way. Let Q be a non-CM non-cuspidal point on $X_0^+(p^3)(\mathbb{Q})$. Let Q_1 be one of its lifts in $Y_0(p^3)(K)$, where K is a quadratic field, and let E be the underlying elliptic curve. By Theorem 8.1 of [5] we still know that $j(Q_1) = j_E$ belongs to $\mathcal{O}_K$. The curve E is endowed with a cyclic isogeny of degree p^3 over K. Proposition 3.3 gives $p^{3/2} \leq 7\cdot 10^3 \max\{\mathrm{h}_{\mathcal{F}}(E), 985\}$. So now either $p \leq (7\cdot 10^6)^{2/3} < 4\cdot 10^4$ and we are done, or $p^{3/2} \leq 7\cdot 10^3 \mathrm{h}_{\mathcal{F}}(E)$. In the latter case Theorem 2.2 implies that $p^{1/2} \leq 7\cdot 10^3(2\log p + 4)$, which can be re-written as $ep^{1/2} \leq 2.8\cdot 10^4 e\log(ep^{1/2})$ (where $e = 2.718\ldots$). Since $x/\log x \geq 2.8\cdot 10^4 e$ for $x \geq 1.1\cdot 10^6$, we obtain $ep^{1/2} < 1.1\cdot 10^6$, which implies $p < 1.7\cdot 10^{11}$, as wanted. □

4 The Heegner-Gross sieve

4.1 Reminder on Mazur's techniques and Heegner-Gross vectors

For the convenience of the reader, we here recall the strategy explained in [26], paragraph 6, improved by the use of generalized jacobians as in the work of Merel ([22]). Those results are used in our algorithm. We refer to [26], [28] and [22] for details. In all what follows, we assume $p \geq 11,\ p \neq 13$.

4.1.1 Variant of Mazur's techniques

Let $r > 1$ an integer and P be a non-cuspidal and non-CM rational point on $X_0^+(p^r)$. The point P gives rise to a point $x \in Y_0(p^r)(K)$ defined over a number field K with $[K:\mathbb{Q}] \leq 2$. By Mazur's results [19], K is quadratic for $p \geq 11, p \neq 13$. Let denote by $\pi_p : X_0(p^r) \longrightarrow X_0(p)$ the natural morphism which preserves the j-invariant. It is easy to see that if the points $x_1 = \pi_p \circ w_{p^r}(x)$ and $x_2 = w_p \circ \pi_p(x)$ are equal in $X_0(p)(K)$, then x is a CM point which yields a contradiction. To study when this equality occurs, we use a variant of techniques developped by Mazur in [20].

Denote by $X_0(p)_{\mathbb{Z}}$ the normalization of $\mathbb{P}^1$ in $X_0(p)$ via $j : X_0(p) \longrightarrow X_0(1) \simeq \mathbb{P}^1$ and by $Y_0(p)_{\mathbb{Z}}$ the open affine subscheme obtained by deleting the cusps. Recall $\mathcal{O}_K$ denotes the ring of integers of K and let $X_0(p)^{\mathrm{sm}}_{\mathcal{O}_K}$ be the smooth part of $X_0(p)_{\mathcal{O}_K} = X_0(p)_{\mathbb{Z}} \times_{\mathbb{Z}} \mathrm{Spec}(\mathcal{O}_K)$ obtained by removing the supersingular points in characteristic p. Let $s_1, s_2 : \mathrm{Spec}(\mathcal{O}_K) \longrightarrow X_0(p)_{\mathcal{O}_K}$ the sections defined by x_1, x_2, respectively. The next Proposition follows from the work of Momose ([24]) and from [26].

Proposition 4.1 *(i) In the fibers of characteristic p, the sections s_1 and s_2 are not supersingular points and coincide ;*

(ii) the field K is a quadratic extension of $\mathbb{Q}$ in which p splits.

In the sequel, we adopt the notations of [22]: we denote by $J_0(p)^\sharp$ the generalized jacobian of $X_0(p)$ with respect to the set of cusps and by $J_e^\sharp$ the *winding quotient* of $J_0(p)^\sharp$. Let $J_0(p)^\sharp_{\mathcal{O}_K}$ and $J_{e\,\mathcal{O}_K}^\sharp$ the respective Néron models over $\mathrm{Spec}(\mathcal{O}_K)$. We consider the composition $\phi_P : Y_0(p) \longrightarrow J_e^\sharp$ of the canonical morphism $J_0(p)^\sharp \longrightarrow J_e^\sharp$ with the Albanese morphism $Y_0(p) \longrightarrow J_0(p)^\sharp$ which to a point Q associates the class of the divisor $[(Q) - (x_1)]$. By Proposition 4.1, one can extend ϕ_P to a morphism

$$\phi_P : Y_0(p)^{\mathrm{sm}}_{\mathcal{O}_K} \longrightarrow J_{e\,\mathcal{O}_K}^\sharp$$

and the images $\phi_P(s_1)$ and $\phi_P(s_2)$ coincide in characteristic p. Since any section of the identity component $J_{e\,\mathcal{O}_K}^{\sharp\,0}$ of $J_{e\,\mathcal{O}_K}^\sharp$ is of finite order (see [22] Proposition 2), it follows that if ϕ_P is a formal immersion at $s_{1/\mathbb{F}_p}$ then $s_1 = s_2$ so $x_1 = x_2$. We refer for instance to [22], Proof of Proposition 6 in Section 4, for a detailed proof of this fact which is a variant of Mazur's techniques [20].

Taking into account the particularity of the fibers in characteristic p of $X_0(p)_{\mathcal{O}_K}$, one can then give a criterion of formal immersion ([26], [22]). Let $\mathcal{S}$ be the finite set of isomorphism classes of supersingular elliptic curves in characteristic p. There is an isomorphism between $\mathrm{Cot}_0(J_0(p)^\sharp_{\mathbb{F}_p})$ and $\mathbb{F}_p^{\mathcal{S}}$. Both can be endowed with a structure of Hecke module compatible with this isomorphism. Any $v = \sum_{s\in\mathcal{S}} \lambda_s[s] \in \mathbb{F}_p^{\mathcal{S}}$ corresponds to an element ω_v of $\mathrm{Cot}_0(J_{e\,\mathbb{F}_p}^\sharp)$ if and only if $I_e^\sharp v = 0$ where we denote by $I_e^\sharp$ the winding ideal of the Hecke algebra (see [22], proof of Proposition 4). Moreover, taking the modular function j as a local parameter for $Y_0(p)_{\mathbb{F}_p}$ in the neighborhood of $s_1/\mathbb{F}_p$, we have $\mathrm{Cot}(\phi_P)(\omega_v) = \sum_{s\in\mathcal{S}} \frac{\lambda_s}{j(P)-j(s)} dj$. It allows to prove the following proposition ([26, 22], see also [21]) .

Proposition 4.2 *Let $s_1 \in Y_0(p)^{\mathrm{sm}}_{\mathbb{Z}_p}(\mathbb{Z}_p)$ be a section, P the point obtained by restriction to the generic fiber and $j(P)$ his j-invariant. Suppose that there exists $v = \sum_{s\in\mathcal{S}} \lambda_s[s] \in \mathbb{Z}^{\mathcal{S}}$ such that $I_e^\sharp v = 0$ and $\sum_{s\in\mathcal{S}} \frac{\lambda_s}{j(P)-j(s)} \neq 0$ in $\mathbb{F}_{p^2}$, then ϕ_P is a formal immersion at $s_{/\mathbb{F}_p}$.*

With the variant of Mazur's techniques explained above, this gives the corollary (see [22] Proposition 6 for this formulation):

Corollary 4.3 ([26, 22]) *If for all ordinary invariant $j_0 \in \mathbb{F}_p$, there exists $v = \sum_{s\in\mathcal{S}} \lambda_s[s] \in \mathbb{Z}^{\mathcal{S}}$ such that $I_e^\sharp v = 0$ and $\sum_{s\in\mathcal{S}} \frac{\lambda_s}{j_0-j(s)} \neq 0$ in $\mathbb{F}_{p^2}$, then $X_0^+(p^r)(\mathbb{Q})$ is trivial for all $r > 1$.*

Remark 4.4 The use of generalized jacobians is not necessary (and was not made in [26] nor in [28]), but it allows to give a neater formulation to the criterion of Proposition 4.6 below. As an illustration, one can check that under this new form it readily gives triviality of $X_0^+(37)(\mathbb{Q})$, for instance, whereas the previous version could not deal with this case and we had to invoke instead peculiar studies of level 37 by Hibino, Murabayashi, Momose and Shimura (cf. [16], [25]), as discussed in Section 6, page 9 of [26].

4.1.2 Heegner-Gross vectors

In [26], the second named author made use of a formula of Gross to exhibit some elements $e_D \in \mathbb{Z}^{\mathcal{S}}$ such that $I_e^\sharp e_D = 0$. Let indeed $-D$ be a quadratic imaginary discriminant and $\mathcal{O}_{-D}$ the order of discriminant $-D$. Let $s \in \mathcal{S}$ be the isomorphism class of a supersingular elliptic curve E_s in characteristic p. The ring $R_s = \mathrm{End}_{\mathbb{F}_{p^2}}(E_s)$ is a maximal order of the quaternion algebra $\mathcal{B}$ ramified at p and ∞. Moreover, the elements of $\mathcal{S}$ are in one-to-one correspondance with the set of maximal orders of $\mathcal{B}$. The quadratic field $L = \mathbb{Q}(\sqrt{-D}) = \mathcal{O}_{-D} \otimes \mathbb{Q}$ embeds in $\mathcal{B}$ if and only if p is ramified or inert in L and we then denote by $h_s(-D)$ the number of optimal embeddings of $\mathcal{O}_{-D}$ in R_s modulo conjugation by $R_s^\times$ (an embedding is optimal if it does not extend to any larger order). We now define

$$e_D = \frac{1}{|\mathcal{O}_{-D}^\times|} \sum_{s\in\mathcal{S}} h_s(-D)[s] \tag{18}$$

which we consider as an element of $\frac{1}{12}\mathbb{Z}^{\mathcal{S}}$.

Proposition 4.5 ([26, 22]) *We have $I_e^\sharp e_D = 0$.*

This is a slightly modified version of Proposition 4.1 of [26] as explained in [22], Proposition 5 and Corollary of Theorem 6 (see Remark 4.4).

The $h_s(-D)$ optimal embeddings of $\mathcal{O}_{-D}$ in R_s modulo conjugation by $R_s^\times$ are in one-to-one correspondence with the pairs (E, f), where E is an elliptic curve with CM by $\mathcal{O}_{-D}$, which are isomorphic to E_s in characteristic p and f is a given isomorphism $\mathcal{O}_{-D} \cong \mathrm{End}(E)$ (see for instance [15]). So for p inert or ramified in L, the vector e_D is the sum of isomorphism classes of elliptic curves which are the reduction in characteristic p of elliptic curves having CM by $\mathcal{O}_{-D}$. The differential associated to e_D is then just equal to the mod p logarithmic derivative:

$$\frac{H'_{-D}(j)}{H_{-D}(j)}dj,$$

where $H_{-D} = \prod_{E;\mathrm{End}(E)\cong\mathcal{O}_{-D}}(X - j(E))$ is the Hilbert class polynomial associated with $-D$. Applying this to Corollary 4.3 we obtain the following criterion (recall we always assume $p \geq 11$, $p \neq 13$).

Proposition 4.6 *If for all ordinary invariant $j_0 \in \mathbb{F}_p$, there exists a quadratic imaginary discriminant $-D < 0$ such that p is inert or ramified in $\mathbb{Q}(\sqrt{-D})$ and $H'_D(j_0) \neq 0$ in $\mathbb{F}_p$, then $X_0^+(p^r)(\mathbb{Q})$ is trivial for all integers $r > 1$.*

4.2 The sieve

We actually use even a more restrictive criterion.

Corollary 4.7 *Let $-D$ be a fundamental quadratic imaginary discriminant and χ_D the associated quadratic Dirichlet character. For a positive integer c, write $R_{c,D} := \mathrm{Res}(H'_{-D}, H'_{-c^2D})$ the integer resultant. Suppose that $p > 11$, $p \neq 13$ is a prime such that $\chi_D(p) = 0$ or -1 and[2] $p \nmid r_D := \gcd(R_{c,D}; c \in [\![2, 7]\!])$. Then $X_0^+(p^r)(\mathbb{Q})$ is trivial for all integer $r > 1$.*

Proof Let p be a prime as in the proposition. Then there exists $c \in [\![2, 7]\!]$ such that $R_{c,D} \neq 0$ mod p. (This range of conductors is of course only motivated by our computational needs.) So for all ordinary $j_0 \in \mathbb{F}_p$ either $H'_{-D}(j_0)$ or $H'_{-c^2D}(j_0)$ is non-zero. Moreover, p is inert or ramified in $\mathbb{Q}(\sqrt{-D})$. The result follows from Proposition 4.6. □

We are now ready to state our algorithm.

ALGORITHM, part I: Fix a bound N and a list $\mathcal{D}$ of quadratic imaginary discriminants: in the sequel, we eventually take $N = 10^{14}$ and choose the discriminants $-D$ of class number $h(-D) \leq 4$ (and also $-D = -87$ which is of class number 6) to obtain Hilbert class polynomials of small degree $\deg(H_{-D}) = h(-D)$. For each $-D \in \mathcal{D}$ we compute the prime factors $\neq 13$ in $[\![11, N-1]\!]$ of r_D. In this way, we construct step by step a list $\mathcal{L}$ of fundamental quadratic imaginary discriminants and a list Bad of prime numbers having the following property:

($\star$) *if $p < N$ is a prime number such that $p \notin \mathsf{Bad}$ and $\chi_d(p) \in \{0, -1\}$ for some $-d \in \mathcal{L}$, then $X_0^+(p^r)(\mathbb{Q})$ is trivial for all $r > 1$.*

We also construct a list Good which is useful within the procedure (see below).

Details:

(i) If the class number is one, then H_{-D} is of degree one and unitary so $H'_{-D} = 1$. We initialize $\mathcal{L}$ to $\mathcal{L} = \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$, and Good and Bad to the empty lists.

[2] We use the "French" notation $[\![a, b]\!]$ for the set of integers x satisfying $a \leq x \leq b$.

(ii) Let $-D \in \mathcal{D}$ not yet in $\mathcal{L}$ and $p \in [\![11, N]\!]$ a prime factor of r_D. If p is not yet in Good nor in Bad, then for all $-d \in \mathcal{L}$ we have $p \nmid r_d$ (if $h(-d) = 1$, it is because $H'_{-d} = 1$ and if $h(-d) > 1$ it follows from the step-by-step construction of $\mathcal{L}$). So, if $\chi_d(p) = 0$ or -1 for some $-d \in \mathcal{L}$, then we put p in the list Good; else we put it in Bad. We add $-D$ to $\mathcal{L}$ and start again to (ii) (unless $\mathcal{L} = \mathcal{D}$).

Results: We take $\mathcal{D}$ to be the list of quadratic imaginary discriminants of class number in $[\![1, 4]\!]$ to which we add -87 (see Appendix) and $N = 10^{14}$. We obtain ($\mathcal{L} = \mathcal{D}$ and) $\mathsf{Bad} = \varnothing$. Thus if a prime $11 \leq p < 10^{14}$, $p \neq 13$ is such that $\chi_D(p) = 0$ or -1 for some $-D \in \mathcal{D}$, then $X_0^+(p^r)(\mathbb{Q})$ is trivial for all $r > 1$.

ALGORITHM, part II: In this part, we construct the list VeryBad of "very bad primes", that is, the primes $11 \leq p < 10^{14}$ which split in $\mathbb{Q}(\sqrt{-D})$ for all $-D \in \mathcal{D} = \mathcal{L}$. For such primes, we indeed cannot establish the triviality of $X_0^+(p^r)(\mathbb{Q})$. For this, we refine the "trial search" naive idea as follows.

(i) We consider a sublist $\mathcal{D}'$ of $\mathcal{D}$ for which we compute explicitely the values of congruences of primes which split for all $-d \in \mathcal{D}'$. In practice, we take

$$\mathcal{D}' = \{-3, -4, -15, -20, -7, -11, -39, -52, -51, -68, -19, -23, -87\}.$$

Since -4 and -3 are in $\mathcal{D}'$, a prime p splits for all $-d \in \mathcal{D}'$ if and only if p is a non-zero square modulo q for all $q \in \mathcal{L}' = \{3, 4, 5, 7, 11, 13, 17, 19, 23, 29\}$. Note that we precisely chose the subset $\mathcal{D}'$ because, except for -4, this is the list of the quadratic imaginary discriminants corresponding to the first nine odd prime numbers. The first twelve discriminants of $\mathcal{D}'$ are of class number not exceeding 4, and -87 is of class number 6. We define

$$M = 3 \times 4 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19 \times 23 \times 29 = 12\,939\,386\,460.$$

There are 1 995 840 values of congruences modulo M which are non-zero squares modulo q for all $q \in \mathcal{L}'$. The representatives in the range $[\![0, M-1]\!]$ of those values make a list $\mathcal{S}$. Concretely, to find $\mathcal{S}$, we make a list of all non-zero squares modulo q for each $q \in \mathcal{L}'$ and use the Chinese Remainder Theorem.

(ii) For each value $a \in \mathcal{S}$ and each integer $p \equiv a \pmod{M}$ in the range $[\![11, N]\!]$, if p is pseudo-prime, we test if $\chi_D(p) = 1$ for all $-D \in \mathcal{D} \backslash \mathcal{D}'$. If it is and if p is indeed prime we put it in VeryBad.

Results: with $\mathcal{D}'$ as before and $N = 10^{14}$, we obtain $\mathsf{VeryBad} = \varnothing$.

The output of this is the following.

Proposition 4.8 *If p is a prime number, $11 \leq p < 10^{14}$ and $p \neq 13$, then $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$ consist of cusps and CM points.*

Together with Theorem 3.2 we obtain Theorem 1.1 of the introduction:

Corollary 4.9 *The same conclusion as for Proposition 4.8 is true for $X_0^+(p^r)(\mathbb{Q})$ with $p \geq 11$, $p \neq 13$ (and $r > 1$).*

Proof (of Proposition 4.8). By Part II of the algorithm, since $\mathsf{VeryBad} = \varnothing$, then any prime $p \geq 11$, $13 \neq p < 10^{14}$ is inert or ramified in $\mathbb{Q}(\sqrt{-D})$ for some $-D \in \mathcal{D}$. We conclude by Part I ($\star$) since $\mathsf{Bad} = \varnothing$. □

Remark 4.10 We close this paper by discussing the cursed level 13. As explained in the introduction, the question of the rational points on $X_0^+(169) \cong X_{\mathrm{split}}(13)$ is the only remaining open case among the $X_0^+(p^r)$ for $r > 1$. We do not prove anything new here, but try to use this "stubbornly

resisting" example (according to Darmon's expression) to illustrate in details many of the tools used all over the paper.

First recall that for all prime p, the Jacobian $J_{\mathrm{nonsplit}}(p)$ of the curve $X_{\mathrm{nonsplit}}(p)$ associated to the normalizer of a nonsplit Cartan subgroup mod p is isomorphic to the newpart $J_0^{+,\mathrm{new}}(p^2)$ of the Jacobian $J_0^+(p^2)$ of $X_0^+(p^2)$ (see [7]). On the other hand, one knows that $J_0^+(p^2)$ decomposes up to isogeny as

$$J_0^+(p^2) \sim J_0(p) \times J_0^{+,\mathrm{new}}(p^2) \sim J_0(p) \times J_{\mathrm{nonsplit}}(p)$$

(see e.g. [24], p. 444). The $J_0(p)$ factor in the above decomposition, and more precisely its $J_0^-(p)$, $J_e(p)$ and $\tilde{J}(p)$ successive subquotients, play a crucial role in our techniques, as they allow to use Mazur's method in order to prove integrality of rational points; as is well-known, the absence of such quotients is one of the main problems with the case of $X_{\mathrm{nonsplit}}(p)$ or $X_0^+(p)$.

Now when $p = 13$ one has $J_0(13) = 0$, so the jacobians of $X_{\mathrm{nonsplit}}(p)$ and $X_{\mathrm{split}}(p)$ are isogenous. (In prime level, this is the only case where this interesting phenomenon occurs, as everything is 0 for $p = 2, 3, 5, 7$, i.e. the other p's for which $g(X_0(p)) = 0$). Actually more is true: Burcu Baran proved by computing explicit equations that the two above curves are actually *isomorphic* over $\mathbb{Q}$ (see [1]). One therefore now faces difficulties of "nonsplit type". Our curve is of genus 3, and its jacobian should be of same rank over $\mathbb{Q}$, so not only Mazur's method, but also Chabauty's method is of no help here. The thirteen quadratic imaginary orders with class number one split, according to the decomposition of the number 13 in them, into seven points in $X_{\mathrm{nonsplit}}(13)(\mathbb{Q})$ and six points in $X_{\mathrm{split}}(13)(\mathbb{Q})$. (The rational cusp of the latter restores the balance with $X_{\mathrm{nonsplit}}(13)$). Galbraith [11] and Baran [1] checked there are no rational points but the trivial ones, in a big box (whose size they do not specify however), but to conclude that there are no point at all we would need some effective Mordell, at least for that particular curve. Our Theorem 2.1 can still be used as an approximation for *integral* points (yielding that their Weil height $\mathrm{h}(j)$ is bounded by 76.4 - this can be lowered by optimizing the estimations in the proof of Theorem 2.1), but again we cannot go further by lack of integrality results... Perhaps the techniques of [6] could be of some help here.

5 Appendix : tables and algorithms

- **Quadratic imaginary discriminants of class number in the range $[\![1, 4]\!]$:**

  Class number 1:
  $-\{3, 4, 7, 8, 11, 19, 43, 67, 163\}$

  Class number 2:
  $-\{20, 24, 40, 52, 15, 88, 35, 148, 51, 232, 91, 115, 123, 187, 235, 267, 403, 427\}$

  Class number 3:
  $-\{23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907\}$

  Class number 4:
  $-\{56, 68, 84, 120, 132, 136, 39, 168, 184, 55, 228, 280, 292, 312, 328, 340, 372, 388, 408, 520, 532, 568, 155, 708, 760, 772, 195, 203, 219, 1012, 259, 291, 323, 355, 435, 483, 555, 595, 627, 667, 715, 723, 763, 795, 955, 1003, 1027, 1227, 1243, 1387, 1411, 1435, 1507, 1555\}$

- **Algorithms** : we reproduce here the pseudo-codes of the algorithms described in Section 4.2. The original codes have been written with Sage [29]. We used the hilbert_class_polynomial function to compute H_{-D} and the crt function to apply Chinese Remainder Theorem.

  Algorithm, Part I:

  bad_discrim_and_primes($\mathcal{D}, N$)

  Require: A list $\mathcal{D}$ of imaginary quadratic discriminants and an integer $N > 1$ (as in Section 4.2).

  1: set $L \leftarrow [3, 4, 7, 8, 11, 19, 43, 67, 163]$, Bad $\leftarrow []$, and Good $\leftarrow []$.
  2: **for** d in $\mathcal{D}$ **do**

3: set $G \leftarrow H'_{-d}$
4: compute the prime factors $\mathcal{P}_D$ of $r_D := \gcd(\mathrm{Res}(G, H'_{-c^2 D}); c \in [\![2, 7]\!])$
5: **for** p in $\mathcal{P}_D$ **do**
6: **if** $p > 10$ and $p < N + 1$ and p not in Good and p not in Bad **then**
7: **if** $\chi_{-m}(p) = 1$ for all m in L **then**
8: add p to the list Bad
9: **else**
10: add p to the list Good.
11: add d to the list L (and go to step 3 with another d in $\mathcal{D}$).
12: **return** $[L, \mathsf{Bad}]$.

Algorithm, Part II:

(i) Let $\mathcal{L}'$ be a list of pairwise coprime moduli $d_1, \ldots, d_n$ and put $M = \mathrm{lcm}(\mathcal{L}') = d_1 \ldots d_n$. The following function returns the non-zero squares modulo all the integers $d_1, \ldots, d_n$ as a list of the form $[M, [\text{integers modulo } M]]$.

squares_congruences($\mathcal{L}'$)

Require: a list $\mathcal{L}'$ of pairwise coprime moduli
1: do a list $[[k^2 \pmod n] \mid k \in \{1, \ldots, (n-1)/2\}] : n \in \mathcal{L}']$
2: **return** [lcm($\mathcal{L}'$), Chinese Remainder Theorem applied to the preceeding list].

(ii) Suppose given a list $C = [M, [s_1, \ldots, s_r]]$ with M a moduli and $s_1, \ldots, s_r$ integers modulo M, a list L of quadratic imaginary discriminants, and two integers n, m with $n < m$. The following function gives the prime numbers in range $[n, m[$ which are congruent to some s_i modulo M and which split in all the quadratic fields with discriminant in L.

very_bad_primes(C, L, n, m)

Require: C, L, n, m as before.
1: $li \leftarrow []$
2: **for** $i \in \{1, \ldots, r\}$ **do**
3: $p \leftarrow s_i + \lceil \frac{n - s_i}{M} \rceil * M$
4: **while** $p < m$ **do**
5: **if** p is pseudoprime and $\chi_{-D}(p) = 1$ for all $D \in L$ **then**
6: **if** p is prime **then**
7: add p to the list li
8: $p \leftarrow p + M$
9: **return** li

Applying the algorithms:

1: set $\mathcal{D}$ to be the list of quadratic imaginary discriminants of class number in range $[\![1, 4]\!]$ to which we add -87, and
set $\mathcal{D}' = \{-3, -4, -15, -20, -7, -11, -39, -52, -51, -68, -19, -23, -87\}$.
2: $[L, \mathsf{Bad}] \leftarrow$ bad_discrim_and_primes($\mathcal{D}, 10^{14}$)
3: $C \leftarrow$ square_congruences($[3, 4, 5, 7, 11, 13, 17, 19, 23, 29]$)
4: $V \leftarrow$ very_bad_primes($C, \mathcal{D} \backslash \mathcal{D}', 11, 10^{14}$)

Result: for any prime $p \in [11, 10^{14}]$ such that $p \notin \mathsf{Bad} \cup V$, the rational points on $X_0^+(p^r)$ are trivial for all integer $r > 1$.

References

[1] *B. Baran*, An exceptional isomorphism between modular curves of level 13, preprint (available on the author's webpage).

[2] *Yu. Bilu*, Baker's method and modular curves, "A Panorama of Number Theory or The View from Baker's Garden" (edited by G. Wüstholz), 73–88, Cambridge University Press, 2002.

[3] *Yu. Bilu, M. Illengo*, Effective Siegel's theorem for modular curves, Bull. London Math. Soc., to appear; `arXiv:0905.0418`.

[4] *Yu. Bilu, P. Parent*, Serre's uniformity problem in the split Cartan case, Ann. Math. (2), **173** (2011), 569–584; `arXiv:0807.4954`.

[5] *Yu. Bilu, P. Parent*, Runge's method and modular curves, Int. Math. Research Notices, July 2010 (electronic); `arXiv:0907.3306`.

[6] *N. Bruin, M. Stoll*, The Mordell-Weil sieve: proving the non-existence of rational points on curves, LMS J. Comput. Math. **13** (2010)

[7] *I. Chen*, Jacobians of modular curves associated to normalizers of Cartan subgroups of level p^n, C. R. Acad. Sci. Paris, Ser. I **339** (2004), 187–192.

[8] *N. Elkies*, On elliptic K-curves. Modular curves and abelian varieties, 81–91, Progr. Math. **224**, Birkhäuser, Basel, 2004.

[9] *G. Faltings*, Endlichkeitsätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **73** (1983), 549–576.

[10] *S. Galbraith*, Rational points on $X_0^+(p)$, Experiment. Math. **8** (1999), 311–318.

[11] *S. Galbraith*, Rational points on $X_0^+(N)$ and quadratic $\mathbb{Q}$-curves, J. Th. Nombres Bordeaux **14** (2002), 205–219.

[12] *É. Gaudron, G. Rémond*, Théorème des périodes et degrés minimaux d'isogénies, manuscript (2011).

[13] *J. Gonzalez*, On the j-invariant of the quadratic $\mathbb{Q}$-curves, J. London Math. Soc. **63** (2001), 52–68.

[14] *B. H. Gross*, Arithmetic of elliptic curves with complex multiplication, L.N.M. **776**, Springer (1980).

[15] *B. H. Gross*, Heights and the special values of L-series. In Number theory (Montreal, Que., 1985), volume **7** of CMS Conf. Proc., pages 115–187. Amer. Math. Soc., Providence, RI, 1987.

[16] *T. Hibino, N. Murabayashi*, Modular equations of hyperelliptic $X_0(N)$ and an application, Acta Arithm. **82** (1997), 279-291.

[17] *D. S. Kubert, S. Lang*, Modular units, Grund. math. Wiss. **244**, Springer, New York-Berlin, 1981.

[18] *D. W. Masser, G. Wüstholz*, Estimating isogenies on elliptic curves, Invent. Math. **100** (1990), 1–24.

[19] *B. Mazur*, Modular curves and the Eisenstein ideal, Publications mathématiques de l'I.H.E.S. **47** (1977), 33–186.

[20] *B. Mazur*, Rational isogenies of prime degree (with an appendix by D. Goldfeld). Invent. Math. **44** (1978), 129–162.

[21] *L. Merel*, Sur la nature non-cyclotomique des points d'ordre fini des courbes elliptiques, avec un appendice de E. Kowalski et Ph. Michel, Duke Math. J. **110** (2001), 81-119.

[22] *L. Merel*, Normalizers of split Cartan subgroups and supersingular elliptic curves, in "Diophantine Geometry" (edited by U. Zannier), pp. 237–255; CRM Series **4**, Edizioni della Normale, Pisa, 2007.

[23] *F. Momose*, Rational points on the modular curves $X_{\mathrm{split}}(p)$, Compositio Math. **52** (1984), 115–137.

[24] *F. Momose*, Rational points on the modular curves $X_0^+(p^r)$, J. Fac. Sci. Univ. Tokyo, Sect. IA, Math. **33** (1986), 441-446.

[25] *F. Momose, M. Shimura*, Lifting of supersingular points on $X_0(p^r)$ and lower bound of ramification index, Nagoya Math. J., Vol. **165** (2002), 159-178.

[26] *P. Parent*, Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$, Compos. Math. **141** (2005), 561–572.

[27] *F. Pellarin*, Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques, Acta Arith. **100** (2001), 203–243.

[28] *M. Rebolledo*, Module supersingulier, formule de Gross-Kudla et points rationnels de courbes modulaires, Pacific J. Math. **234** (2008), 167–184.

[29] http://www.sagemath.org/

[30] *J.-P. Serre*, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), 259–331.

[31] *J. H. Silverman*, Heights and elliptic curves, *in* Arithmetic geometry, G. Cornell and J. H. Silverman (eds.), Springer, New-York, 1984, 253–265.